UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF NORTH CAROLINA WESTERN DIVISION
Civil Action No.

GREGORY VOGEL, individually and on behalf of all others similarly situated, Plaintiff, v. **ADVANCE AUTO PARTS, INC.,** Defendant.	**CLASS ACTION COMPLAINT FOR DAMAGES** [Jury Trial Demanded]

CLASS ACTION COMPLAINT

Plaintiff Gregory Vogel brings this action individually, and on behalf of all others similarly situated, by and through counsel, against Defendant Advance Auto Parts, Inc. ("Defendant" or "Advance Auto"), for its failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") stored within Defendant's information network.

Plaintiff makes these allegations on personal information as to those allegations pertaining to himself and his personal circumstances, and upon information and belief, based on the investigation of counsel and facts that are matters publicly known, on all other matters.

INTRODUCTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach"). On information and belief, the Data Breach has impacted over 67,000 individuals.[1]

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of

[1] https://cybernews.com/news/advance-auto-parts-confirms-breach/ (last visited June 26, 2024)

former and current employees and job applicants' highly sensitive personal identifiable information ("PII").

3. In a recent SEC filing, Defendant confirmed that their data was stolen from a third-party cloud database environment:

> On May 23, 2024, Advance Auto Parts, Inc. (the "Company") identified unauthorized activity within a third-party cloud database environment containing Company data and launched an investigation with industry-leading experts. On June 4, 2024, a criminal threat actor offered what it alleged to be Company data for sale. The Company has notified law enforcement.[2]

4. After investigating the stolen files, Defendant states "[it] believes [the stolen files] contain personal information for current and former employees and job applicants, including social security numbers and other government identification numbers."[3]

5. Advance Auto is a leading automotive parts provider that operates thousands of stores across the US and has reported revenue exceeding $11 billion.[4] In the regular course of its business, Advance Auto is required to maintain reasonable and adequate security measures to secure, protect, and safeguard their customers' PII against unauthorized access and disclosures.

6. Defendant's current and former employees and job applicants, like Plaintiff and Class Members, provided certain PII to Defendants, which is necessary to obtain employment with Defendant.

7. Large companies like Defendant have an acute interest in maintaining the confidentiality of the PII entrusted to it, and they are well-aware of the numerous data breaches that have occurred throughout the United States and their responsibility for safeguarding PII in

---

[2] https://www.sec.gov/Archives/edgar/data/1158449/000115844924000162/aap-20240523.htm (last visited June 26, 2024)

[3] *Id*.

[4] https://cybernews.com/news/advance-auto-parts-confirms-breach/ (last visited June 26, 2024)

their possession.

8. Plaintiff and Class Members entrusted Defendant with, and allowed Defendant to gather, highly sensitive information as part of obtaining employment. They did so in confidence, and they had the legitimate expectation that Defendant would respect their privacy and act appropriately, including only sharing their information with vendors and business associates who legitimately needed the information and were equipped to protect it through having adequate processes in place to safeguard it.

9. Every year, millions of Americans have their most valuable PII stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to make the necessary investments to implement important and adequate security measures to protect their customers' data.

10. Defendant required its current and former employees and job applicants to provide it with their sensitive PII and failed to protect it. Defendant had an obligation to secure its customers' PII by implementing reasonable and appropriate data security safeguards.

11. As a result of Defendant's failure to provide reasonable and adequate data security, Plaintiff and the Class Members' unencrypted, non-redacted PII has been exposed to unauthorized third parties. Plaintiff and the Class are now at much higher risk of identity theft and cybercrimes of all kinds, especially considering the highly sensitive PII stolen here. This risk constitutes a concrete injury suffered by Plaintiff and the Class, as they no longer have control over their PII, which PII is now in the hands of third- party cybercriminals. This substantial and imminent risk of identity theft has been recognized by numerous courts as a concrete injury sufficient to establish standing.

12. Furthermore, Plaintiff and the Class, as also set forth below, will have to incur costs

to pay a third-party credit and identity theft monitoring service for the rest of their lives as a direct result of the Data Breach.

13. Plaintiff brings this action on behalf of himself and those similarly situated to seek redress for the lifetime of harm they will now face, including, but not limited to reimbursement of losses associated with identity theft and fraud, out-of-pocket costs incurred to mitigate the risk of future harm, compensation for time and effort spent responding to the Data Breach, the costs of extending credit monitoring services and identity theft insurance, and injunctive relief requiring Defendant to ensure that its third-party vendors implement and maintain reasonable data security practices going forward.

THE PARTIES

14. Plaintiff Gregory Vogel is a natural person and a resident of Ohio who completed an online job application with Advance Auto from his home in Hamilton, Ohio.

15. Defendant Advance Auto Parts, Inc. is registered as a domestic North Carolina corporation with its principal place of business at 2626 Glenwood Ave., Ste. 550, Raleigh, North Carolina 27608.

16. Advance Auto advertises itself as a leading automotive aftermarket parts provider which operates over 5,000 stores and Worldpac branches in the United States, Canada, Puerto Rico and the U.S. Virgin Islands, and employs at least 67,000 team members.[5]

17. The true names and capacities of persons or entities, whether individual, corporate, associate or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Plaintiff.

[5] https://jobs.advanceautoparts.com/us/en/ (last visited June 26, 2024)

18. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of the responsible parties when their identities become known.

JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Plaintiff and Defendant are citizens of different states.

20. This Court has personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District and does substantial business in this District.

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because Defendant's principal office is in this District and because a substantial part of the events or omissions giving rise to the claim occurred in this District

STATEMENT OF FACTS

Defendant's Data Breach

22. Plaintiff is a former job applicant of Advance Auto.

23. As a condition of the job application process with Advance Auto, applicants were required to disclose their PII to Defendant and its subsidiaries, including but not limited to, their names, social security numbers, and dates of birth. Defendant used that PII to facilitate Plaintiff's job application and required Plaintiff to provide that PII to obtain employment with Advance Auto.

24. On information and belief, Advance Auto collects and maintains former and current employees and job applicants' unencrypted PII in its computer systems.

25. In collecting and maintaining the PII, Advance Auto implicitly agrees it will

safeguard the data using reasonable means according to its internal policies and federal law.

26. In a recent SEC filing, Advance Auto confirmed that their data was stolen from a third-party cloud database environment:

> On May 23, 2024, Advance Auto Parts, Inc. (the "Company") identified unauthorized activity within a third-party cloud database environment containing Company data and launched an investigation with industry-leading experts. On June 4, 2024, a criminal threat actor offered what it alleged to be Company data for sale. The Company has notified law enforcement.[6]

27. After investigating the stolen files, Defendant states "[it] believes [the stolen files] contain personal information for current and former employees and job applicants, including social security numbers and other government identification numbers."[7]

28. In June 2024, Advance Auto issued a Data Breach Notice (the "Notice") to notify impacted individuals of the Data Breach.

Plaintiff Vogel's Experience

29. In the course of completing the online job application, Plaintiff was required to provide his PII to Defendant, including his name, social security number, date of birth, address, and contact information.

30. Plaintiff provided his PII to Advance Auto and trusted that the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

31. As a result, Plaintiff's information was among the data accessed by an unauthorized third party in the Data Breach.

---

[6] https://www.sec.gov/Archives/edgar/data/1158449/000115844924000162/aap-20240523.htm (last visited June 26, 2024)

[7] *Id*.

32. At all times herein relevant, Plaintiff is and was a member of the Class.

33. As a result of the Data Breach, Plaintiff was injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring his accounts with heightened scrutiny, time spent dealing with increased spam emails, and time spent seeking legal counsel regarding his options for remedying and/or mitigating the effects of the Data Breach.

34. Plaintiff was also injured by the material risk to future harm he suffers based on the Defendant's Data Breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the Data Breach, the data involved is highly sensitive and presents a high risk of identity theft or fraud.

35. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII that he entrusted to Defendant, and which was compromised in and as a result of the Data Breach.

36. Plaintiff, as a result of the Data Breach, has increased anxiety about his loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling his PII.

37. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name, being placed in the hands of unauthorized third parties/criminals.

38. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in the Defendant's possession, is protected and safeguarded from future breaches.

Defendant Collected/Stored Class Members' PII

39. Defendant acquired, collected, stored, and assured reasonable security over Plaintiff's and Class Members' PII.

40. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII.

41. Defendant, in turn, stored that information in the part of Defendant's computer and information system that was ultimately affected by the Data Breach.

42. By obtaining, collecting, and storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties to protect that PII and knew or should have known that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

43. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

44. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized use of this information.

45. Defendant represented to current and former employees, job applicants and the public that they possess robust security features to protect PII and that it takes its responsibility to protect PII seriously.

46. Defendant could have prevented the Data Breach, which began no later than May 23, 2024, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII.

47. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII is exacerbated by repeated warnings, and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

48. Yet, despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

49. In 2023, 3,502 data breaches occurred, resulting in over 353,000,000 individuals impacted.[8]

50. In light of recent high profile data breaches at other industry leading companies, including MOVEIt (17.5 Million Records, June 2023), LastPass/GoTo Technologies (30 Million Records, August 2022), Neopets (69 Million Records, July 2022), WhatsApp (500 million records, November 2022), Twitter (5.4 Million records, July 2022), Cash App (8.2 Million Users, April 2022), LinkedIn (700 Million Records, April 2021), Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

51. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses

[8] https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last visited June 26, 2024)

to obtain PII." The FBI further warned that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[9]

52. Moreover, the Defendant was, or should have been, aware of the foreseeable risk of a cyberattack, like the one it experienced. In fact, Advance Auto experienced a previous data breach in 2019 which exposed financial information of up to 56,000 of its customers.[10]

53. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Advance Auto.

Defendant failed to adhere to FTC guidelines

54. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

55. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

[9] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-thefinancial-sector (last visited June 26, 2024)

[10] https://www.fenderbender.com/running-a-shop/operations/article/33022974/advance-auto-parts-releases-info-on-computer-breach-at-14-stores (last visited June 26, 2024)

56. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

57. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

58. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

59. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers, or in this case former and current employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

60. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[11]

61. In addition to its obligations under federal and state laws, Defendant owed a duty

[11] The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

Defendant Failed to Comply with Industry Standards

62. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

63. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices.

64. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices.

65. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center

for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

66. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant Had an Obligation to Protect the Stolen Information

67. Defendant's failure to adequately secure Plaintiff's and Class Members' sensitive PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

68. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

69. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, networks, and personnel policies and procedures to ensure that the PII was adequately secured and protected.

70. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

71. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

72. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

73. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

74. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

75. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

76. PII are valuable commodities for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

77. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information is sold at prices ranging from $40 to $200, and bank details have a price range of $50 to $200.[12] Criminals also can purchase access to entire sets of information

[12] Your Personal Data Is for Sale on the Dark Web. Here's How Much It Costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-onthe-dark-web-how-much-it-costs/ (Last visited June 26, 2024)

obtained from company data breaches for prices ranging from $900 to $4,500.[13]

78. Social Security numbers are among the worst kinds of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

79. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[14]

80. In addition, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against potential misuse of a Social Security number is not permitted; an individual instead must show evidence of actual, ongoing fraud to obtain a new number.[15]

81. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

---

[13] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymousbrowsing/in-the-dark (Last visited June 26, 2024).
[14] Social Security Administration, Identity Theft and Your Social Security Number, available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (Last visited June 26, 2024).
[15] Bryan Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-shackers-has-millionsworrying-about-identity-theft (Last visited June 26, 2024).

82. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, in that situation, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—name, birthdate, and Social Security number.

83. This data commands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

84. Identity thieves can use PII, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

85. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used: according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot

[16] Time Greene, Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers, IT World, (Feb. 6, 2015), available at: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10xprice-of-stolen-credit-card-numbers.html (Last visited June 26, 2024)

necessarily rule out all future harm.[17]

86. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

87. he Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

88. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiffs' and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

Common Injuries & Damages Suffered by the Plaintiff and Putative Class

89. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is present and

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed June 26, 2024).

continuing, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and (e) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

90. Plaintiff and Class Members are at a heightened risk of identity theft for years to come. The link between a data breach and the risk of identity theft is simple and well-established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft-related crimes discussed below.

91. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet, the resource and asset of time has been lost.

92. Plaintiff and Class Members have spent and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

93. These efforts are consistent with the U.S. Government Accountability Office report in 2007 regarding data breaches in which it noted that victims of identity theft will face

"substantial costs and time to repair the damage to their good name and credit record."[18]

94. These efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[19]

95. The value of the PII of the Plaintiff and Class Members is valuable.[20] Its value is axiomatic, considering the value of Big Data in corporate America and the criminal consequences of cyber thefts, which include significant prison sentences and fines. Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has a considerable market value.

96. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[21]

97. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any

[18] See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf ("GAO Report"). (last visited June 26, 2024)

[19] *Id*.

[20] See, e.g., Randall T. Soma, et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted) (Last visited June 26 2024).

[21] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited June 26, 2024).

consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the PII has been lost, thereby causing additional loss of value.

98. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

99. There is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

100. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. And fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

101. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

CLASS ACTION ALLEGATIONS

102. Plaintiff, individually and on behalf of others similarly situated, seeks to certify the following class and subclasses of similarly situated persons under Rule 23 of the Federal Rules of Civil Procedure:

Nationwide Class. All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach (the "Class").

103. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their immediate families and members of their staff.

104. Plaintiff reserves the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

105. **Numerosity.** A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class (which Plaintiff is informed and believe, and on that basis, alleges that the total number of persons exceeds hundreds of thousands of individuals) are so numerous that joinder of all members is impractical, if not impossible.

106. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

a. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether the Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

107. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

108. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's counsel is competent and experienced in litigating class actions.

109. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' PII was stored on the same computer network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

110. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual

Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

111. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

COUNT I
Negligence
(On behalf of Plaintiff and the Class against Defendant)

112. Plaintiff realleges paragraphs 1–111 as if fully set forth herein.

113. Plaintiff and members of the Class entrusted their PII to Advance Auto. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the PII of Plaintiff and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

114. Advance Auto was under a basic duty to act with reasonable care when it undertook to collect, create, maintain, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, inter alia, the Restatement (Second) of

Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

115. Defendant knew that the PII of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harm that could happen if the PII of Plaintiff and the Class was wrongfully disclosed.

116. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

117. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's PII.

118. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII/PHI would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the personal data of Plaintiff and the Class and all resulting damages.

119. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII. Defendant knew its systems and

technologies for processing and securing the PII of Plaintiff and the Class had numerous security vulnerabilities.

120. Defendant was in the sole position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and Class Members had entrusted to it.

121. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

122. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

123. Further, through its failure to provide clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

124. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered by Plaintiff and Class Members.

125. Plaintiff's and Class Members' PII was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

126. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

127. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or

theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to, efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

128. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

129. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Negligence Per Se
(On Behalf of Plaintiff and the Class against Defendant)

130. Plaintiff realleges paragraphs 1–111 as if fully set forth herein.

131. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

132. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII/PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII/PHI.

133. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

134. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

135. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

136. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

137. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft;

(ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

138. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

139. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

140. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT III
Violation of North Carolina Unfair Trade Practices Act
(On behalf of Plaintiff and the Class against Defendant)

141. Plaintiff realleges paragraphs 1–111 as if fully set forth herein.

142. Defendant advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

143. Defendant engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, as set forth above.

144. Defendant's omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII.

145. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its omissions.

146. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Defendant accepted the PII that Plaintiff and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

147. Defendant acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff's and Class members' rights.

148. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

149. Defendant's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

150. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class against Defendant)

151. Plaintiff realleges paragraphs 1–111 as if fully set forth herein.

152. Defendant required Plaintiff and Class Members to provide their PII as a condition of obtaining employment. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant wherein Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their PII had been breached and compromised or stolen.

153. Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

154. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

155. Defendant further entered into an implied contract with Plaintiff and the Class Members to honor its representations and assurances regarding protecting their PII.

156. Plaintiff and Class Members fully performed their obligations under implied contracts with Defendant.

157. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

158. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

159. Defendant, through its own actions and omissions breached the implied contracts it made with Plaintiff and Class Members by (i) failing to implement technical, administrative, and physical security measures to protect the PII from unauthorized access or disclosure, despite such measures being readily available, (ii) failing to limit access to the PII to those with legitimate

reasons to access it, (iii) failing to store the PII only on servers kept in a secure, restricted area, and (iv) otherwise failing to safeguard the PII.

160. In these and other ways, Defendant violated its duty of good faith and fair dealing.

161. As a direct and proximate result of Defendant's breach of its implied contract, Plaintiff and Class Members are at a substantial, impending, and imminent risk of identity theft, and they have been forced to take mitigation steps, thereby incurring costs, to ensure their personal and financial safety.

162. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic damages in the following forms: (a) financial costs incurred mitigating the imminent risk of identity theft; (b) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft; (c) financial costs incurred due to actual identity theft; (d) the cost of future identity theft monitoring; (e) loss of time incurred due to actual identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PII.

163. As a direct and proximate result of the above-described breaches of implied contract, Plaintiff and Class Members are entitled to recover actual, consequential, and nominal damages.

COUNT V
Invasion of Privacy – Intrusion Upon Seclusion
(On Behalf of Plaintiff and the Class against Defendant)

164. Plaintiff realleges paragraphs 1–111 as if fully set forth herein.

165. Plaintiff and Class Members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

166. Defendant intruded upon that seclusion by allowing the unauthorized access to the Plaintiff and Class Members' PII without Plaintiff and Class Members' consent, knowledge, authorization, notice, or privilege by negligently maintaining the confidentiality of Plaintiff and Class Members' information as set out above.

167. Defendant's breach of confidentiality resulted in insecure systems allowing harmful disclosure of the information to criminals and criminal data markets.

168. The intrusion was offensive and objectionable to Plaintiff, the Class Members and to a reasonable person or ordinary sensibilities in that Plaintiff and Class Members' PII was disclosed without prior written authorization of Plaintiff and the Class.

169. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class Members provided and disclosed their PII to Defendants privately with the intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without consent. Plaintiff and the Class Members were further reasonable to believe that the PII would be reasonably protected against third-party criminal extraction through foreseeable hacking activity.

170. This improper disclosure increased the risk that the personal data was delivered to criminal data markets thereby increasing the risk of identity theft to Plaintiff and the Class Members.

171. As a direct and proximate result of Defendant's unauthorized disclosure, Plaintiff and Class Members have suffered actual and concrete injuries and will suffer additional injuries into the future, including economic and non-economic damages in the following forms: (a) invasion of privacy; (b) financial costs incurred mitigating the imminent risk of identity theft; (c) loss of time and loss of productivity incurred mitigating the imminent risk of identity theft, including medical identity theft; (d) loss of time and loss of productivity taking steps to mitigate the data breach, including the instructions in the Data Breach Letter; (e) the cost of future monitoring for identity theft; (f) loss of time and annoyance due to increased targeting with phishing attempts and fraudulent robo-calls; and (g) diminution of value of their PII.

172. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach

COUNT VI
Unjust Enrichment
(On Behalf of Plaintiff and the Class against Defendant)

173. Plaintiff realleges paragraphs 1–111 as if fully set forth herein.

174. This claim is pleaded in the alternative to the breach of implied contract claim.

175. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII.

176. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

177. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and

Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

178. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards

179. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

180. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

181. Plaintiff and Class Members have no adequate remedy at law.

182. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of

the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

183. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, prays for judgment against Defendant and in Plaintiff's favor, as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as the Class Representative and undersigned counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

e) For an award of punitive damages, as allowable by law;

f) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

g) Pre- and post-judgment interest on any amounts awarded; and,

h) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: June 26, 2024

Respectfully Submitted,

/s/ Joel R. Rhine
Joel R. Rhine (16028)
Ruth A. Sheehan (48069)
John A. Bruno (54775)
Rhine Law Firm, P.C.
1612 Military Cutoff, Suite 300
Wilmington, NC 28403
Tel: (910) 772-9960
Fax: (910) 772-9062
jrr@rhinelawfirm.com
ras@rhinelawfirm.com
jab@rhinelawfirm.com
Local Rule 83.1(d) Attorney

Marc E. Dann (Ohio Bar No. 0039425)*
**Special Appearance pursuant to L.R. 83.1(d) anticipated*
DannLaw
15000 Madison Avenue
Lakewood, OH 44107
Phone: (216) 373-0539
Facsimile: (216) 373-0536
notices@dannlaw.com

Thomas A. Zimmerman, Jr.*
**Special Appearance pursuant to L.R. 83.1(d) anticipated*
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
Fax: (312) 440-4180
tom@attorneyzim.com

Attorneys for Plaintiff and the proposed Class